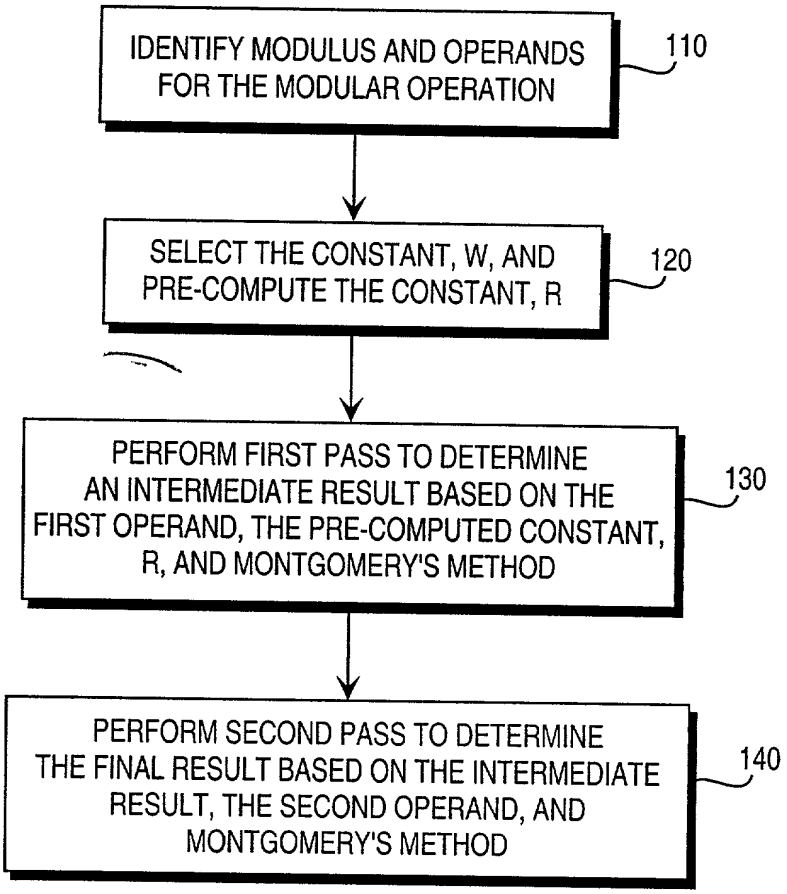

IDENTIFY MODULUS AND OPERANDS FOR THE MODULAR OPERATION
110
SELECT THE CONSTANT, W, AND PRE-COMPUTE THE CONSTANT, R
120
PERFORM FIRST PASS TO DETERMINE AN INTERMEDIATE RESULT BASED ON THE FIRST OPERAND, THE PRE-COMPUTED CONSTANT, R, AND MONTGOMERY'S METHOD
130
PERFORM SECOND PASS TO DETERMINE THE FINAL RESULT BASED ON THE INTERMEDIATE RESULT, THE SECOND OPERAND, AND MONTGOMERY'S METHOD
140

FIG. 1

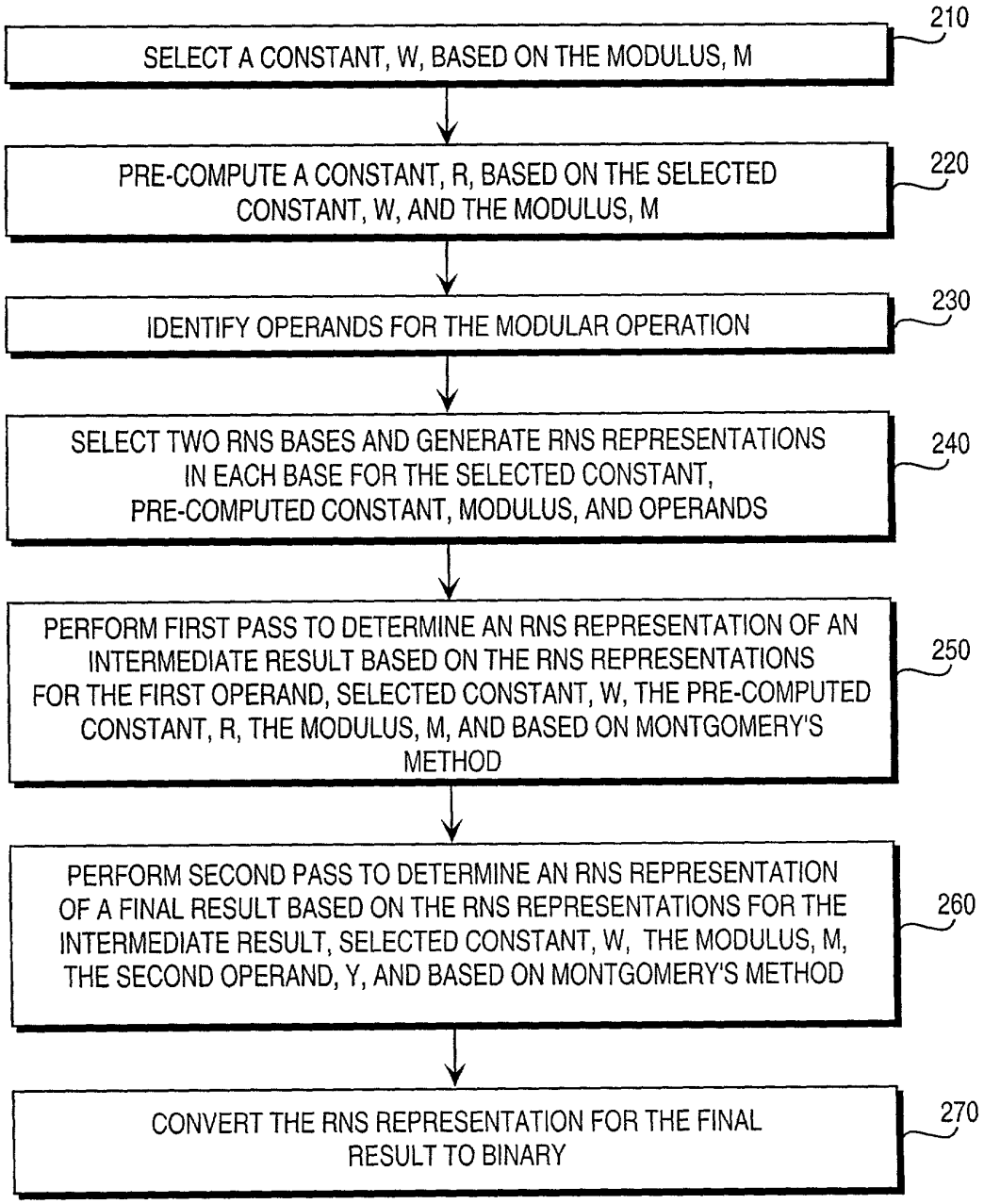

SELECT A CONSTANT, W, BASED ON THE MODULUS, M
210
PRE-COMPUTE A CONSTANT, R, BASED ON THE SELECTED CONSTANT, W, AND THE MODULUS, M
220
IDENTIFY OPERANDS FOR THE MODULAR OPERATION
230
SELECT TWO RNS BASES AND GENERATE RNS REPRESENTATIONS IN EACH BASE FOR THE SELECTED CONSTANT, PRE-COMPUTED CONSTANT, MODULUS, AND OPERANDS
240
PERFORM FIRST PASS TO DETERMINE AN RNS REPRESENTATION OF AN INTERMEDIATE RESULT BASED ON THE RNS REPRESENTATIONS FOR THE FIRST OPERAND, SELECTED CONSTANT, W, THE PRE-COMPUTED CONSTANT, R, THE MODULUS, M, AND BASED ON MONTGOMERY'S METHOD
250
PERFORM SECOND PASS TO DETERMINE AN RNS REPRESENTATION OF A FINAL RESULT BASED ON THE RNS REPRESENTATIONS FOR THE INTERMEDIATE RESULT, SELECTED CONSTANT, W, THE MODULUS, M, THE SECOND OPERAND, Y, AND BASED ON MONTGOMERY'S METHOD
260
CONVERT THE RNS REPRESENTATION FOR THE FINAL RESULT TO BINARY
270

FIG. 2

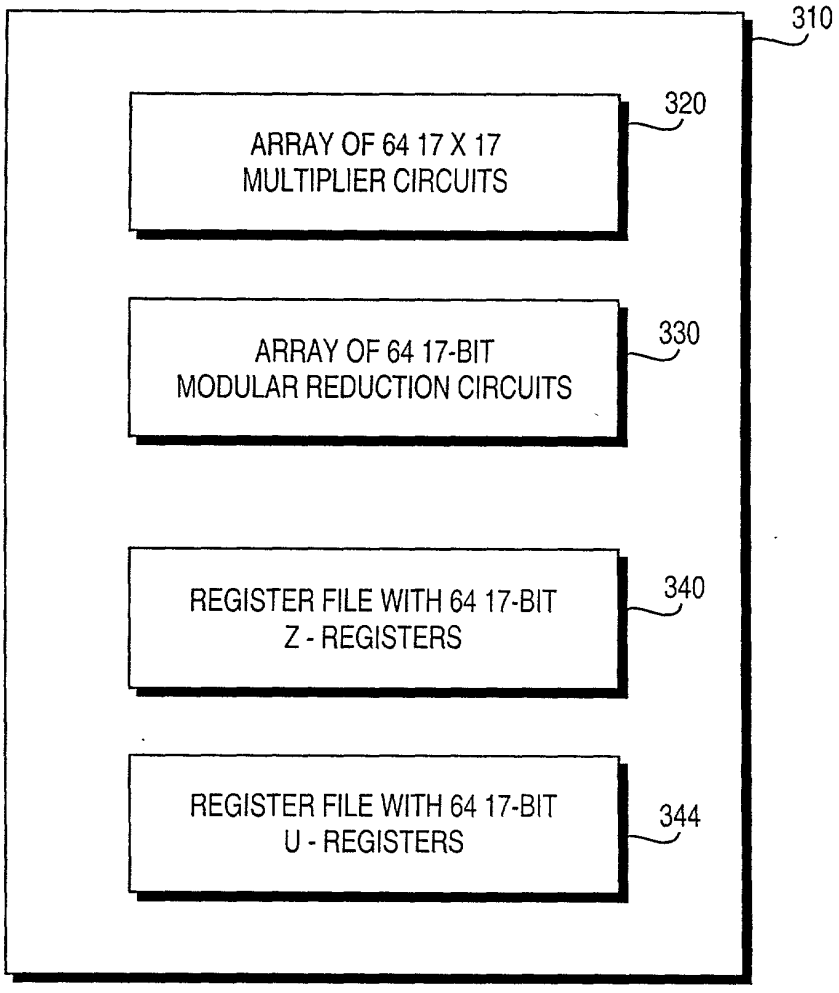

310
320
ARRAY OF 64 17 X 17
MULTIPLIER CIRCUITS
330
ARRAY OF 64 17-BIT
MODULAR REDUCTION CIRCUITS
340
REGISTER FILE WITH 64 17-BIT
Z - REGISTERS
344
REGISTER FILE WITH 64 17-BIT
U - REGISTERS

FIG. 3A

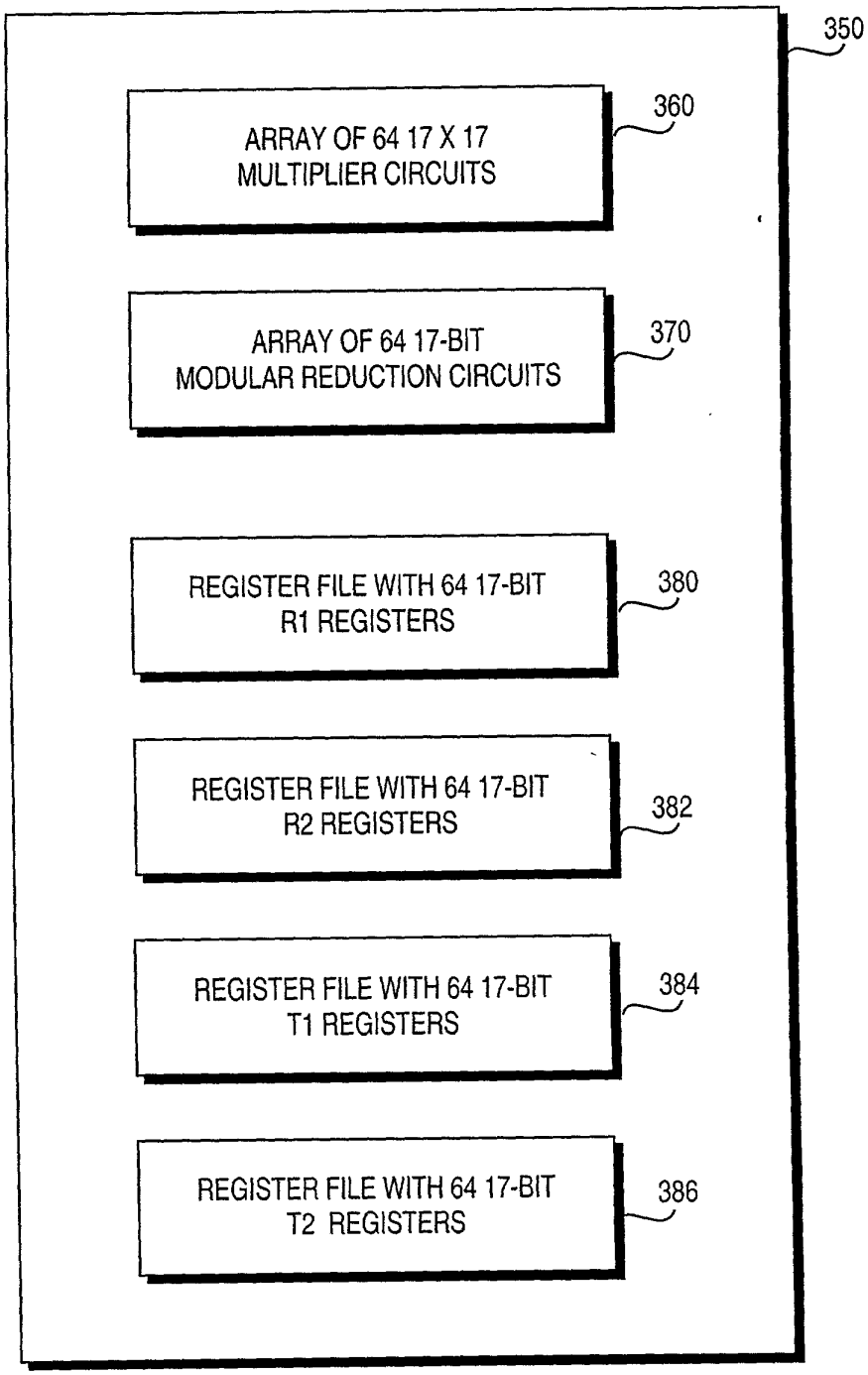

350
ARRAY OF 64 17 X 17 MULTIPLIER CIRCUITS
360
ARRAY OF 64 17-BIT MODULAR REDUCTION CIRCUITS
370
REGISTER FILE WITH 64 17-BIT R1 REGISTERS
380
REGISTER FILE WITH 64 17-BIT R2 REGISTERS
382
REGISTER FILE WITH 64 17-BIT T1 REGISTERS
384
REGISTER FILE WITH 64 17-BIT T2 REGISTERS
386

FIG. 3B

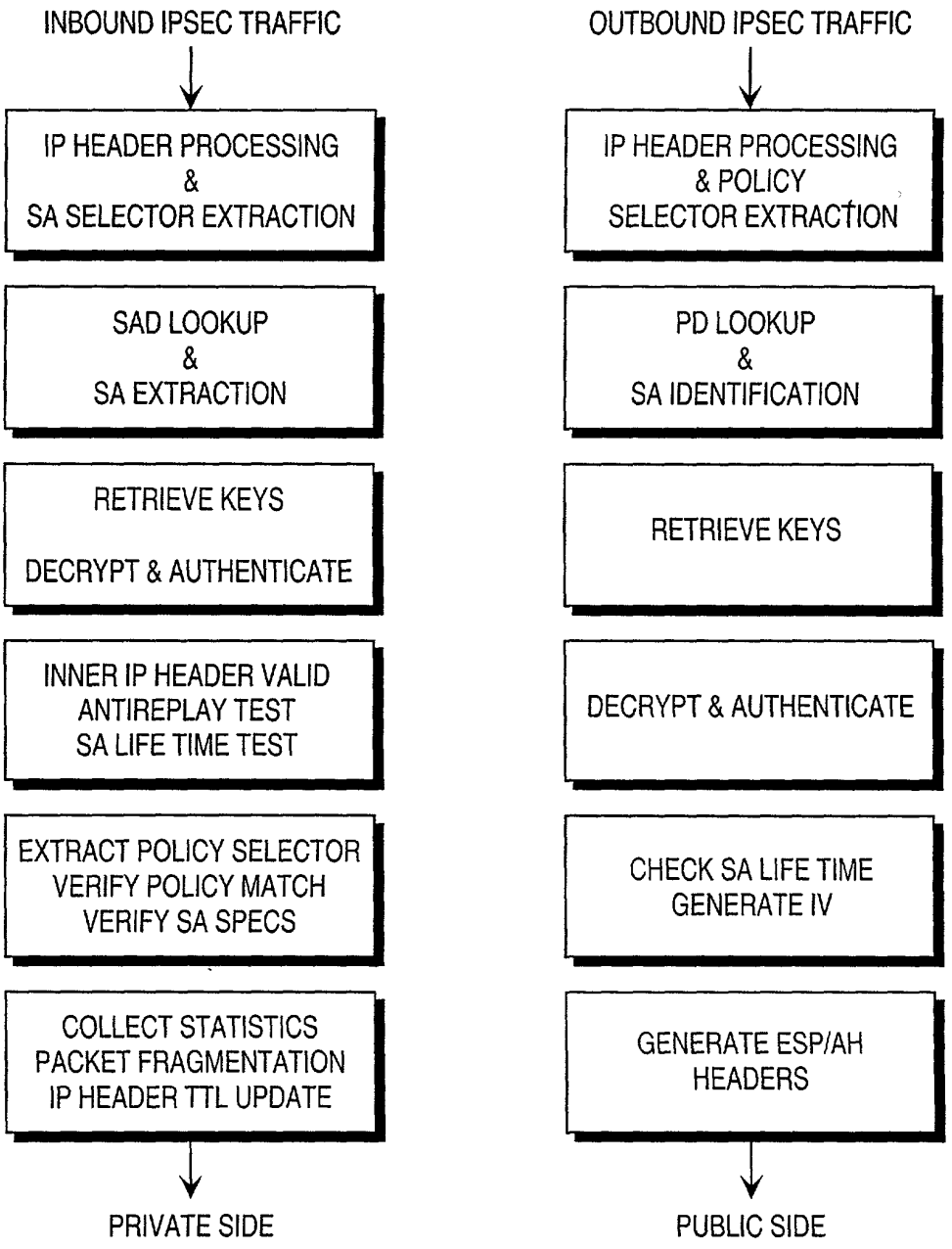

INBOUND IPSEC TRAFFIC
IP HEADER PROCESSING & SA SELECTOR EXTRACTION
SAD LOOKUP & SA EXTRACTION
RETRIEVE KEYS
DECRYPT & AUTHENTICATE
INNER IP HEADER VALID
ANTIREPLAY TEST
SA LIFE TIME TEST
EXTRACT POLICY SELECTOR
VERIFY POLICY MATCH
VERIFY SA SPECS
COLLECT STATISTICS
PACKET FRAGMENTATION
IP HEADER TTL UPDATE
PRIVATE SIDE
OUTBOUND IPSEC TRAFFIC
IP HEADER PROCESSING & POLICY SELECTOR EXTRACTION
PD LOOKUP & SA IDENTIFICATION
RETRIEVE KEYS
DECRYPT & AUTHENTICATE
CHECK SA LIFE TIME
GENERATE IV
GENERATE ESP/AH HEADERS
PUBLIC SIDE

FIG. 4

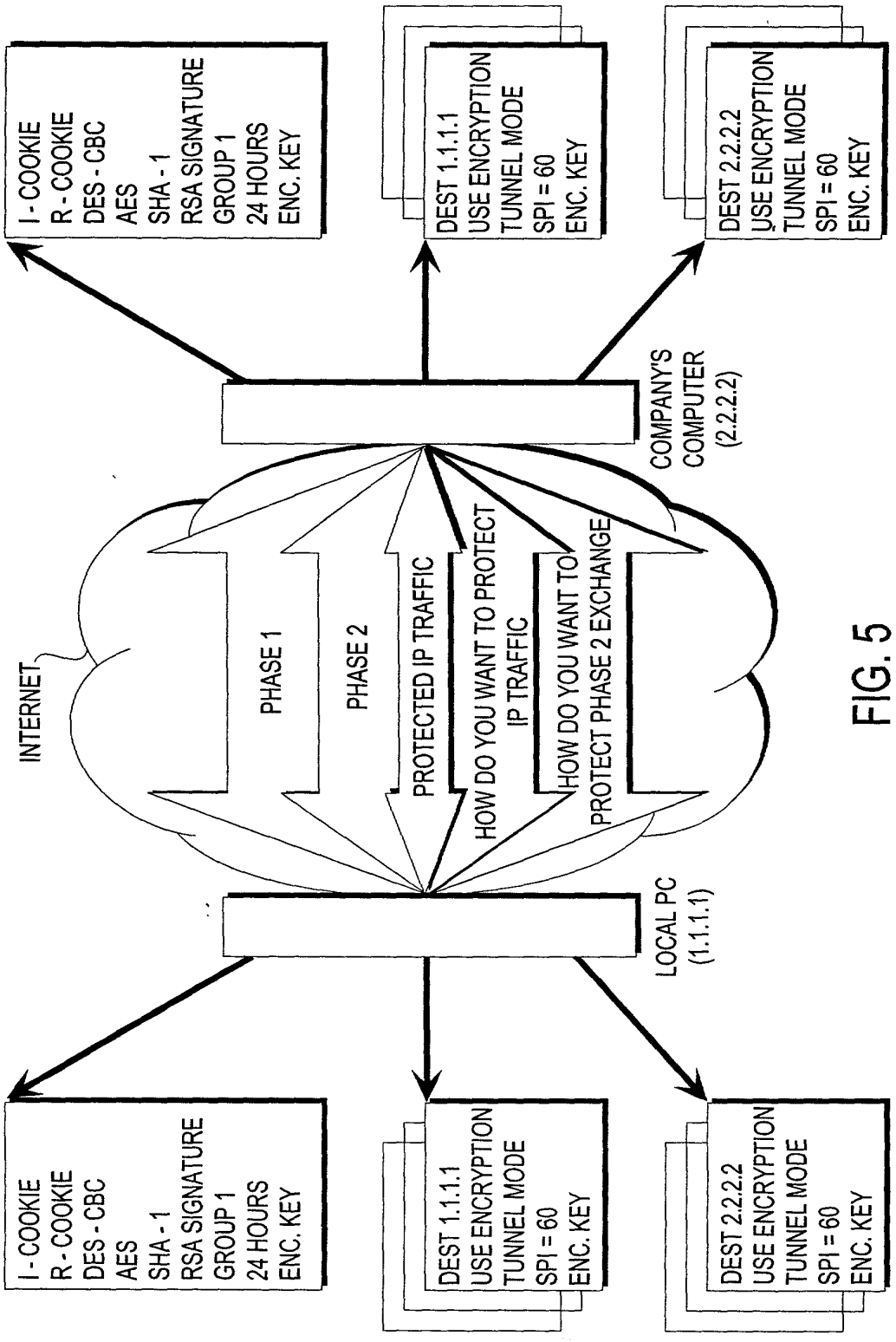

I - COOKIE
R - COOKIE
DES - CBC
AES
SHA - 1
RSA SIGNATURE
GROUP 1
24 HOURS
ENC. KEY
DEST 1.1.1.1
USE ENCRYPTION
TUNNEL MODE
SPI = 60
ENC. KEY
DEST 2.2.2.2
USE ENCRYPTION
TUNNEL MODE
SPI = 60
ENC. KEY
COMPANY'S COMPUTER (2.2.2.2)
INTERNET
PHASE 1
PHASE 2
PROTECTED IP TRAFFIC
HOW DO YOU WANT TO PROTECT IP TRAFFIC
HOW DO YOU WANT TO PROTECT PHASE 2 EXCHANGE
LOCAL PC (1.1.1.1)
I - COOKIE
R - COOKIE
DES - CBC
AES
SHA - 1
RSA SIGNATURE
GROUP 1
24 HOURS
ENC. KEY
DEST 1.1.1.1
USE ENCRYPTION
TUNNEL MODE
SPI = 60
ENC. KEY
DEST 2.2.2.2
USE ENCRYPTION
TUNNEL MODE
SPI = 60
ENC. KEY

FIG. 5

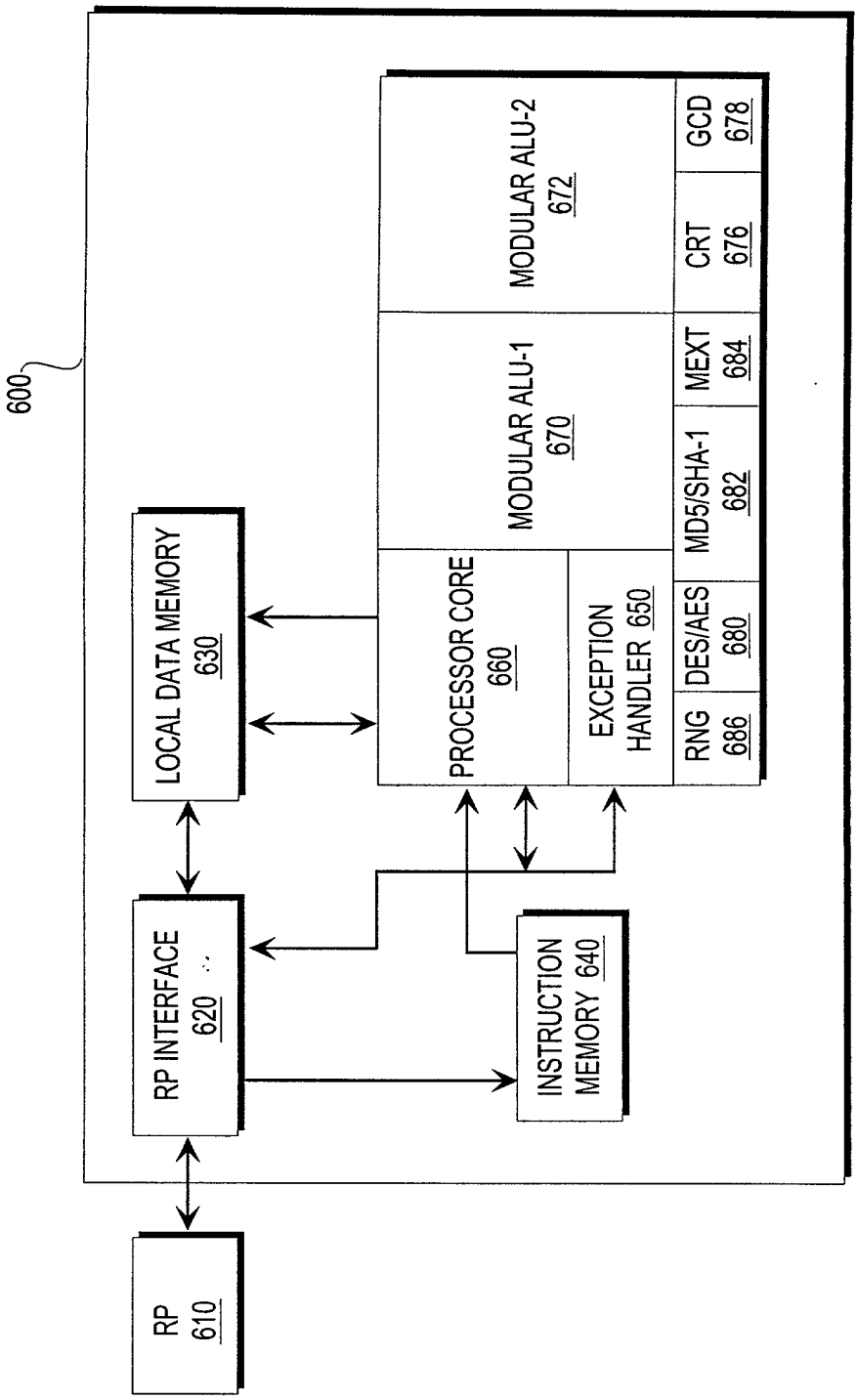

600
RP
610
RP INTERFACE
620
LOCAL DATA MEMORY
630
INSTRUCTION MEMORY
640
PROCESSOR CORE
660
EXCEPTION HANDLER
650
MODULAR ALU-1
670
MODULAR ALU-2
672
RNG
686
DES/AES
680
MD5/SHA-1
682
MEXT
684
CRT
676
GCD
678

FIG. 6

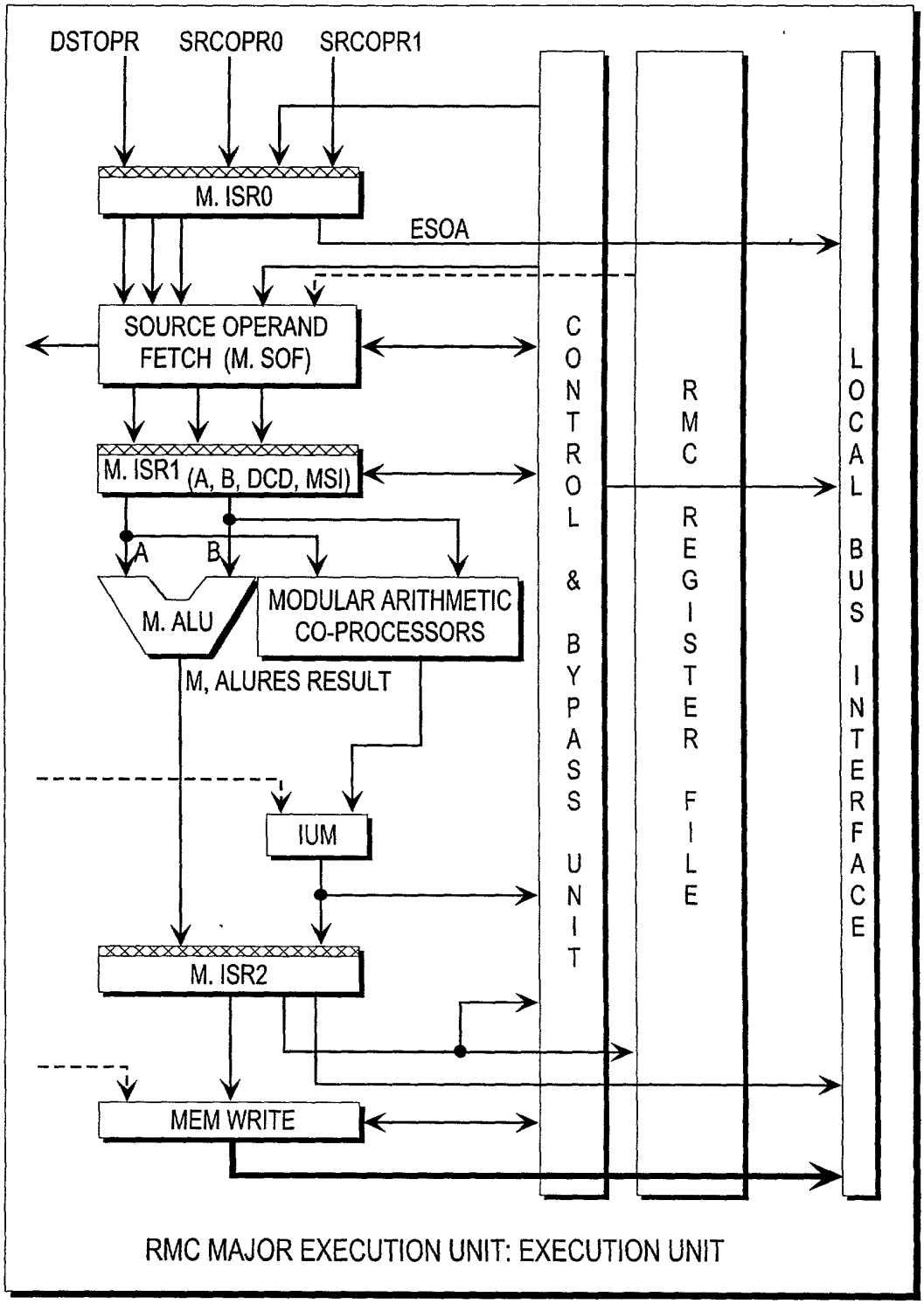


FIG. 7

NOTE: RECTANGULAR BLOCKS ON THE SAME HORIZONTAL LEVEL OVERLAP EXECUTION TIMES.

⇐- SOURCE OVERWRITES DESTINATION REGISTER
®- MODULAR MULTIPLICATION WITH RESPECT TO W.
©- MODULAR MULTIPLICATION WITH RESPECT TO V.
∠- RNS CONVERSION

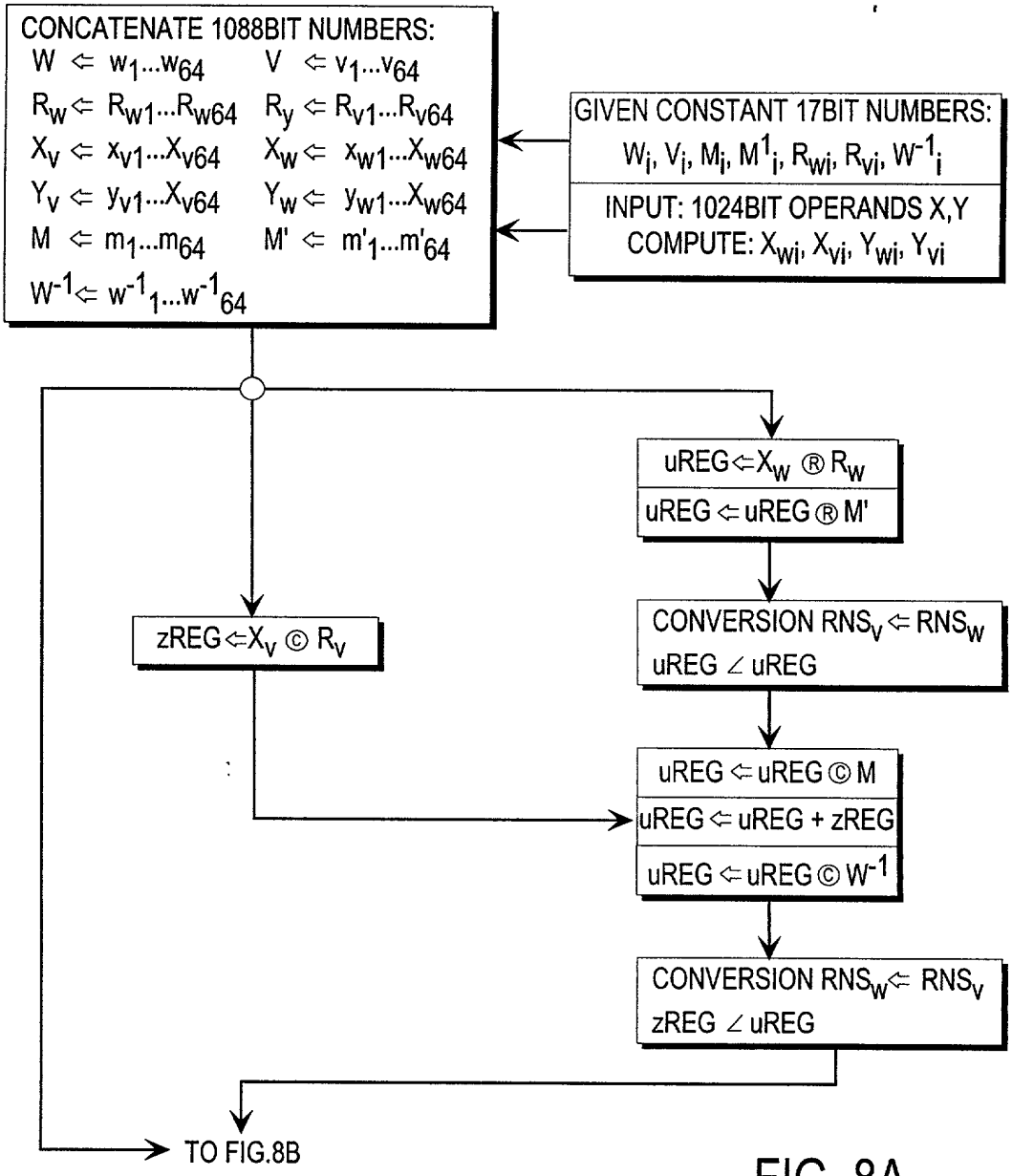


FIG. 8A

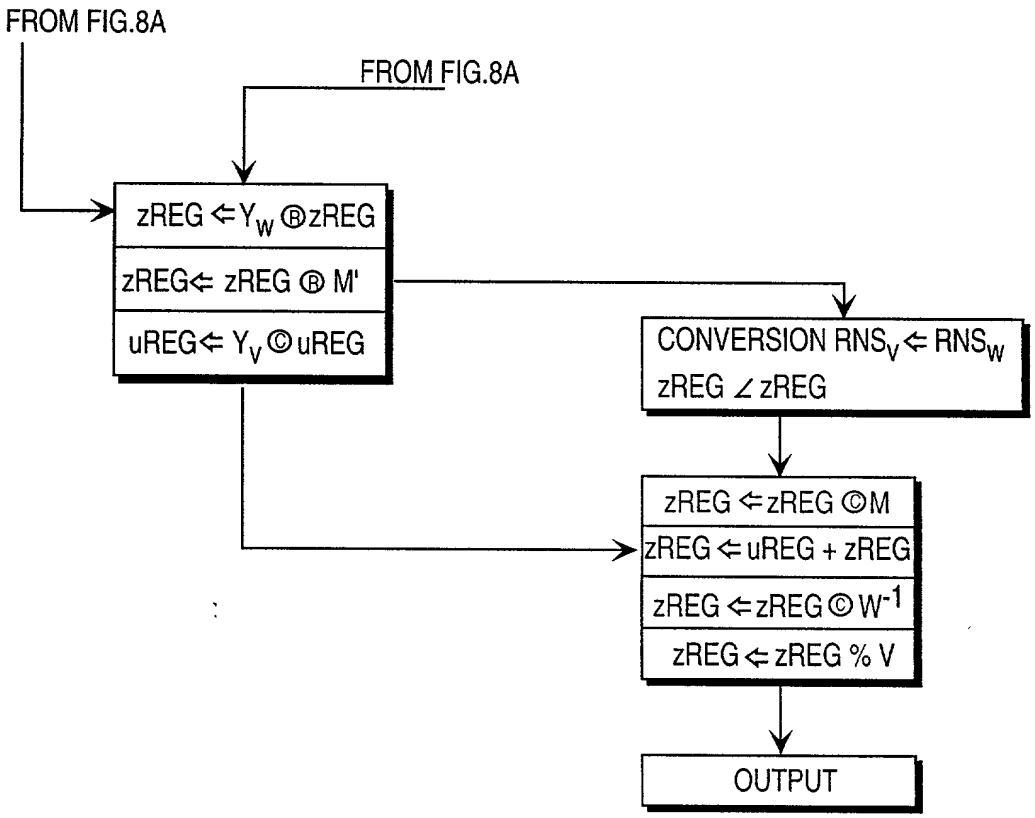

FROM FIG.8A
FROM FIG.8A
zREG ⇐ Y_W ® zREG
zREG⇐ zREG ® M'
uREG⇐ Y_V © uREG
CONVERSION RNS_V ⇐ RNS_W
zREG ∠ zREG
zREG ⇐ zREG © M
zREG ⇐ uREG + zREG
zREG ⇐ zREG © W^{-1}
zREG ⇐ zREG % V
OUTPUT

FIG. 8B

NOTE: ALL BUSSES ARE 64 X 17 = 1088 BITS WIDE.

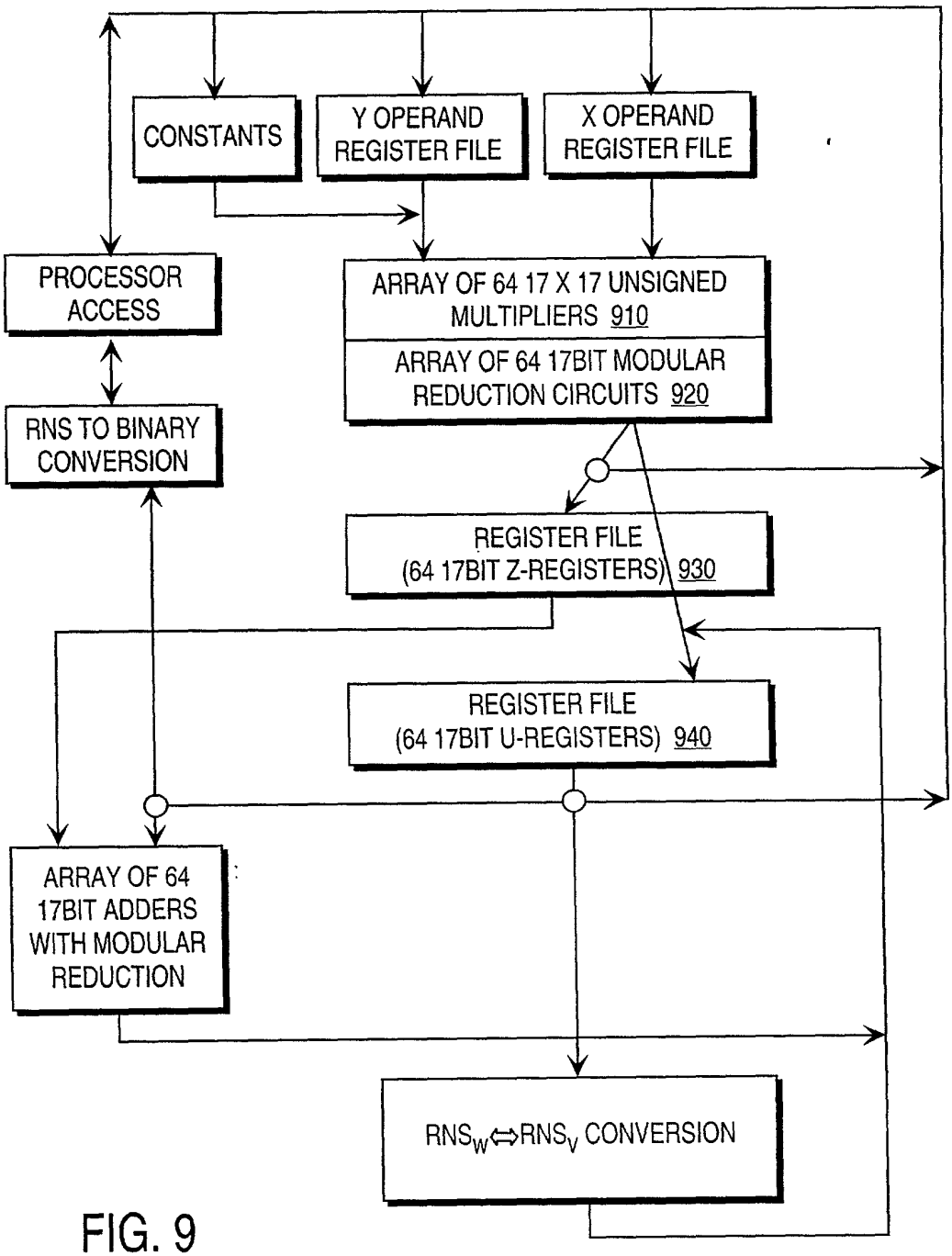


FIG. 9

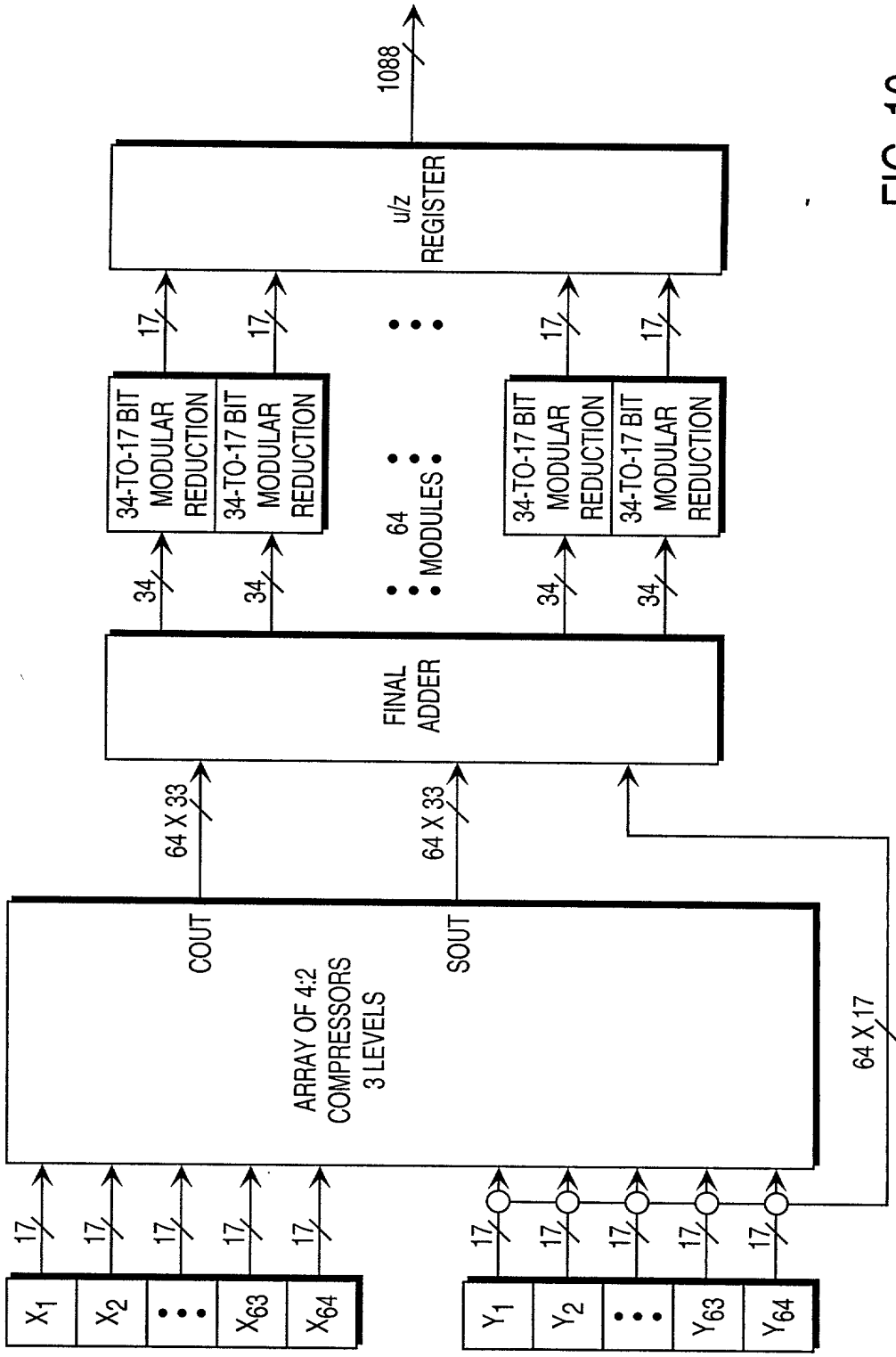


FIG. 10

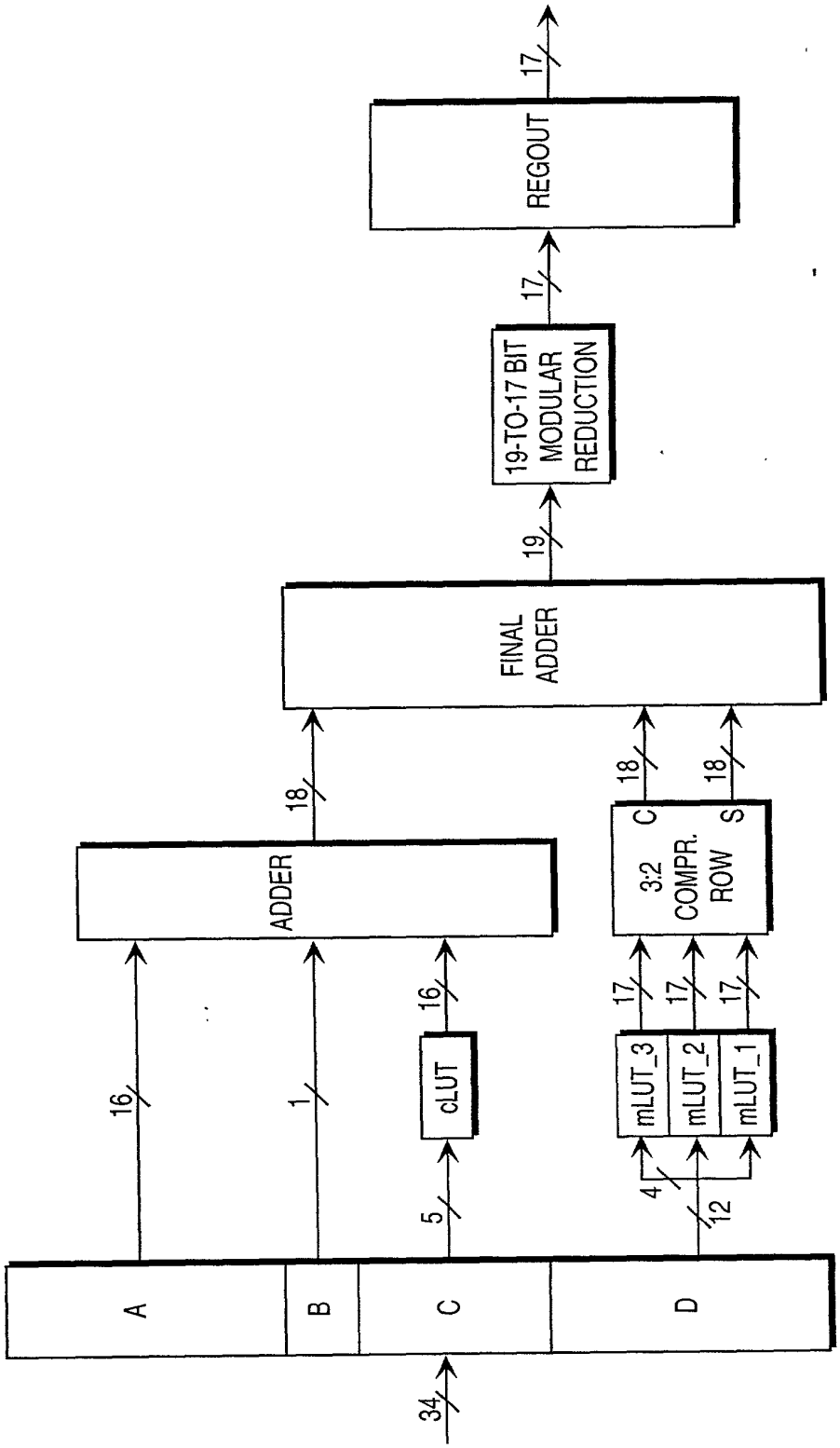
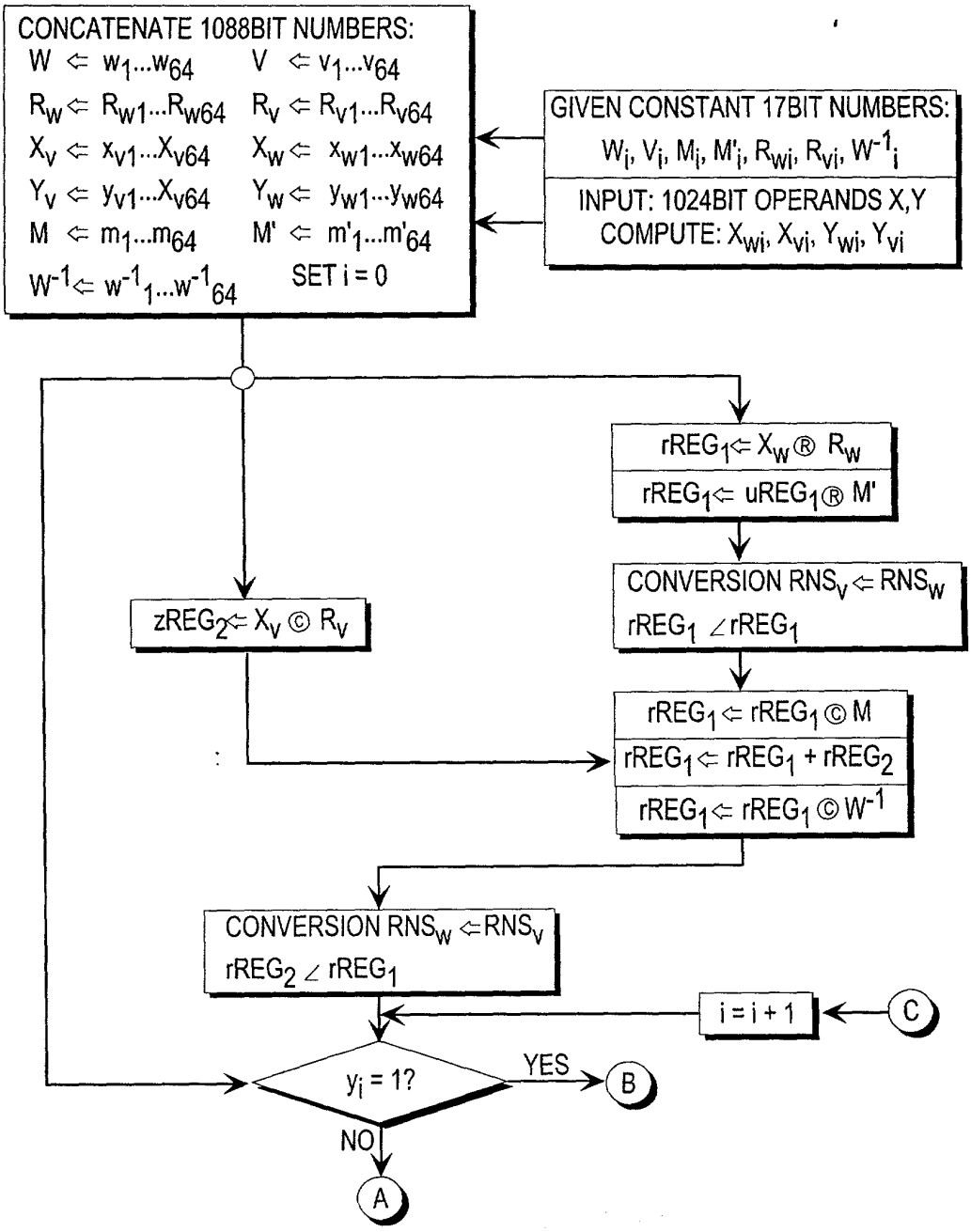


FIG. 11

NOTE: RECTANGULAR BLOCKS ON THE SAME HORIZONTAL LEVEL OVERLAP EXECUTION TIMES.

⇦- SOURCE OVERWRITES DESTINATION REGISTER
®- MODULAR MULTIPLICATION WITH RESPECT TO W.
©- MODULAR MULTIPLICATION WITH RESPECT TO V.
∠- RNS CONVERSION

FIG. 12A



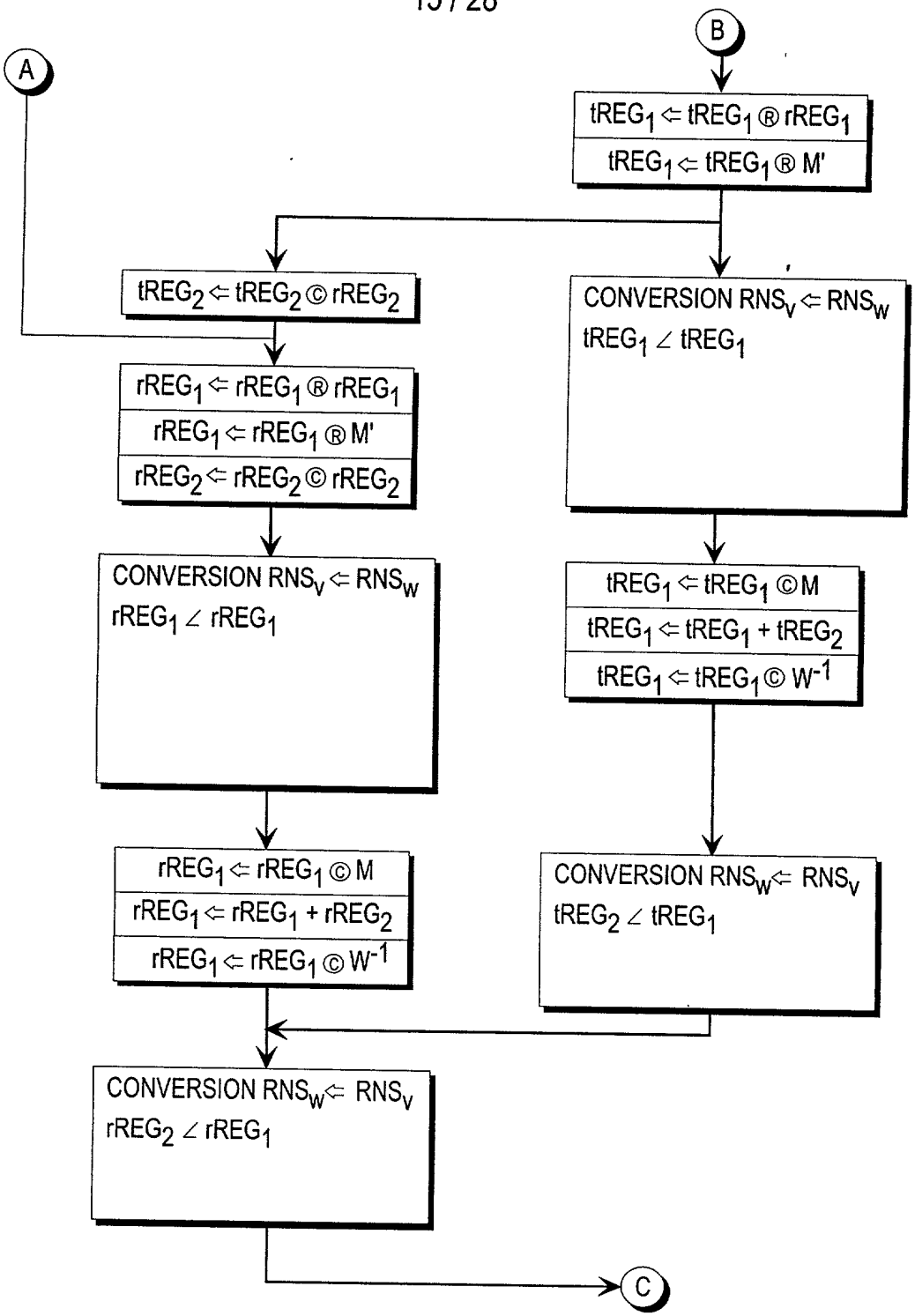

A
B
$tREG_1 \Leftarrow tREG_1 \circledR rREG_1$
$tREG_1 \Leftarrow tREG_1 \circledR M'$
$tREG_2 \Leftarrow tREG_2 \copyright rREG_2$
CONVERSION $RNS_V \Leftarrow RNS_W$
$tREG_1 \angle tREG_1$
$rREG_1 \Leftarrow rREG_1 \circledR rREG_1$
$rREG_1 \Leftarrow rREG_1 \circledR M'$
$rREG_2 \Leftarrow rREG_2 \copyright rREG_2$
CONVERSION $RNS_V \Leftarrow RNS_W$
$rREG_1 \angle rREG_1$
$tREG_1 \Leftarrow tREG_1 \copyright M$
$tREG_1 \Leftarrow tREG_1 + tREG_2$
$tREG_1 \Leftarrow tREG_1 \copyright W^{-1}$
$rREG_1 \Leftarrow rREG_1 \copyright M$
$rREG_1 \Leftarrow rREG_1 + rREG_2$
$rREG_1 \Leftarrow rREG_1 \copyright W^{-1}$
CONVERSION $RNS_W \Leftarrow RNS_V$
$tREG_2 \angle tREG_1$
CONVERSION $RNS_W \Leftarrow RNS_V$
$rREG_2 \angle rREG_1$
C

FIG. 12B

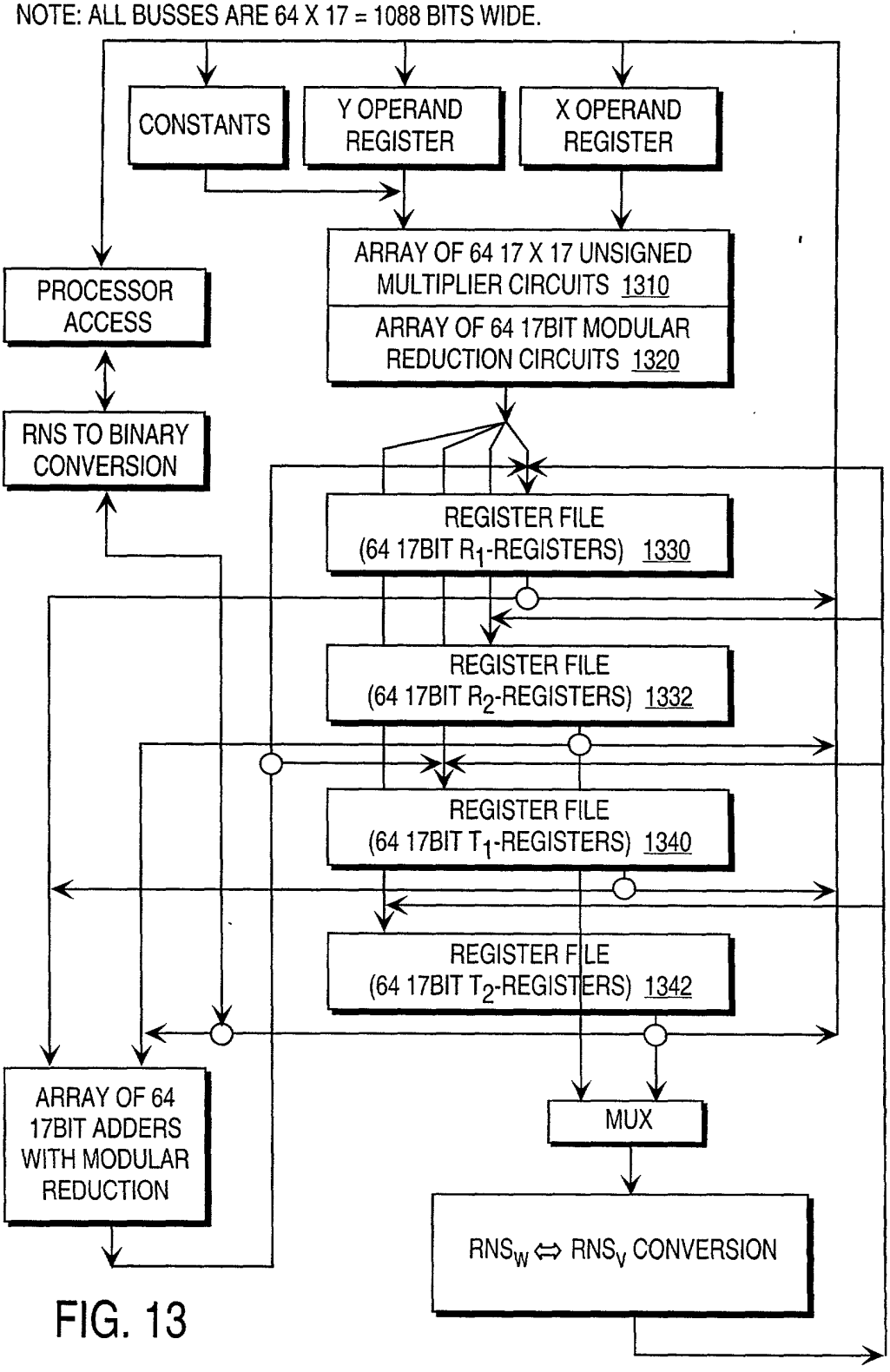

NOTE: ALL BUSSES ARE 64 X 17 = 1088 BITS WIDE.
CONSTANTS
Y OPERAND REGISTER
X OPERAND REGISTER
ARRAY OF 64 17 X 17 UNSIGNED MULTIPLIER CIRCUITS 1310
ARRAY OF 64 17BIT MODULAR REDUCTION CIRCUITS 1320
PROCESSOR ACCESS
RNS TO BINARY CONVERSION
REGISTER FILE (64 17BIT R_1-REGISTERS) 1330
REGISTER FILE (64 17BIT R_2-REGISTERS) 1332
REGISTER FILE (64 17BIT T_1-REGISTERS) 1340
REGISTER FILE (64 17BIT T_2-REGISTERS) 1342
ARRAY OF 64 17BIT ADDERS WITH MODULAR REDUCTION
MUX
$RNS_W \Leftrightarrow RNS_V$ CONVERSION

FIG. 13

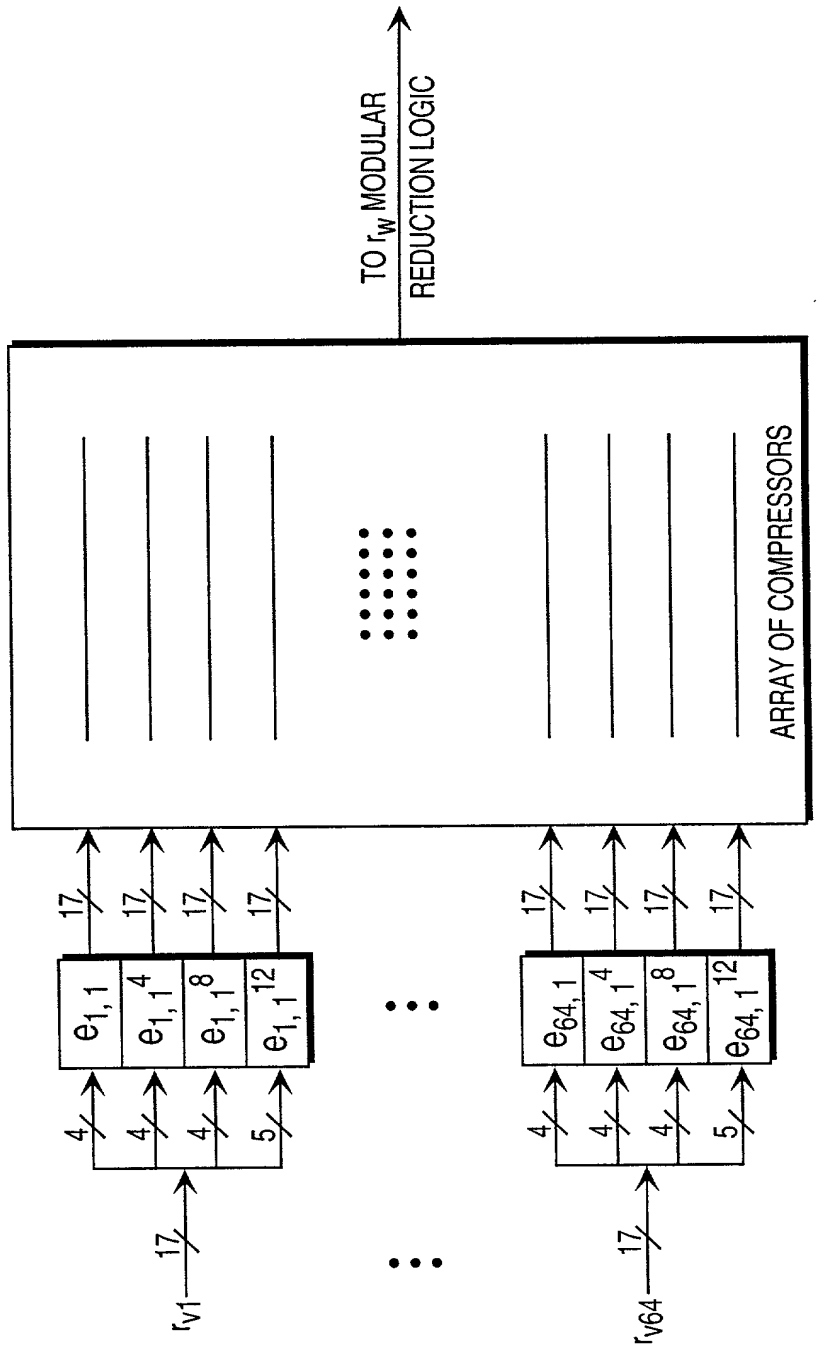


FIG. 14

SINGLE RAW COMPUTATION (SRC) MODULE

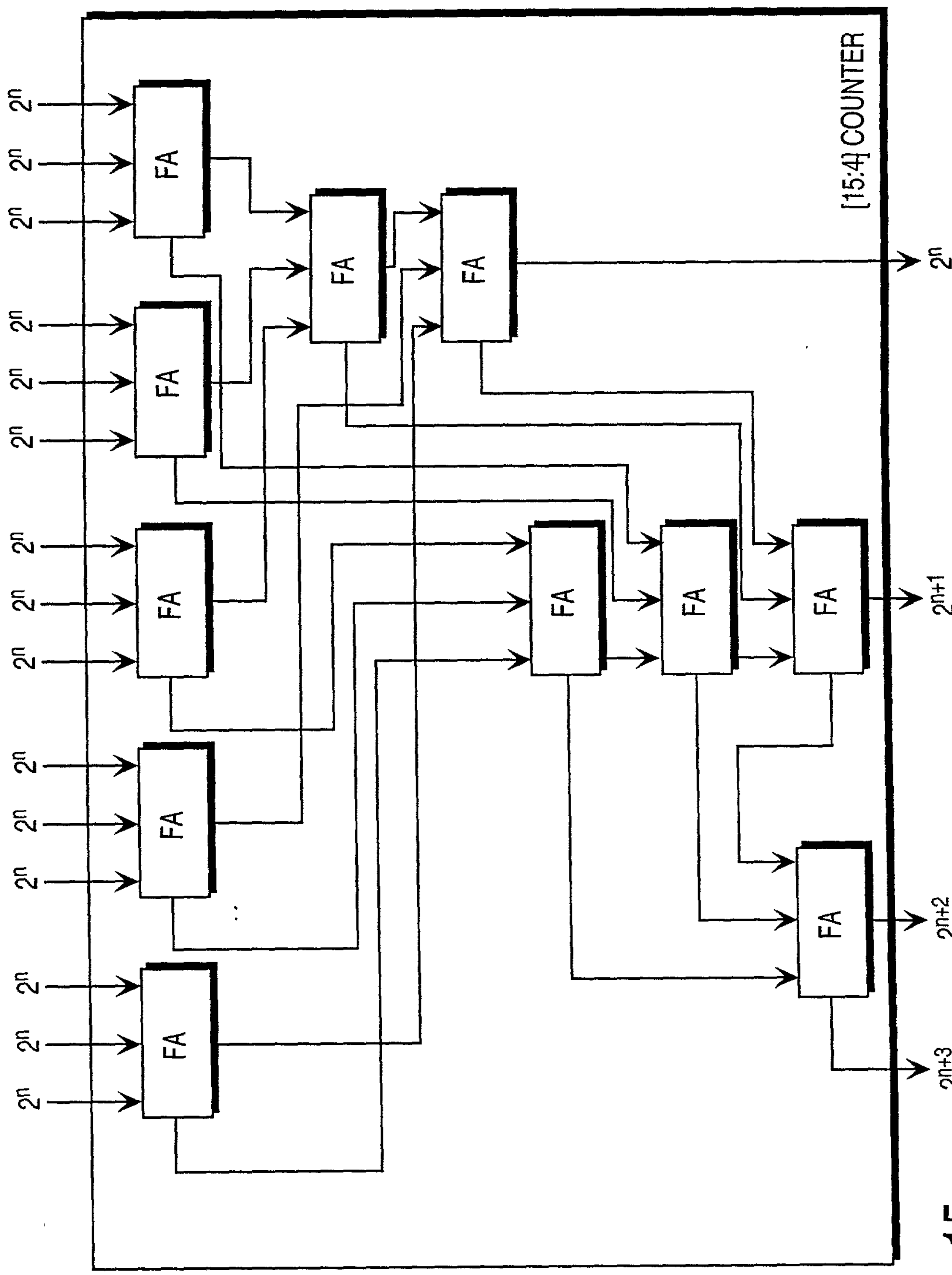


FIG. 15

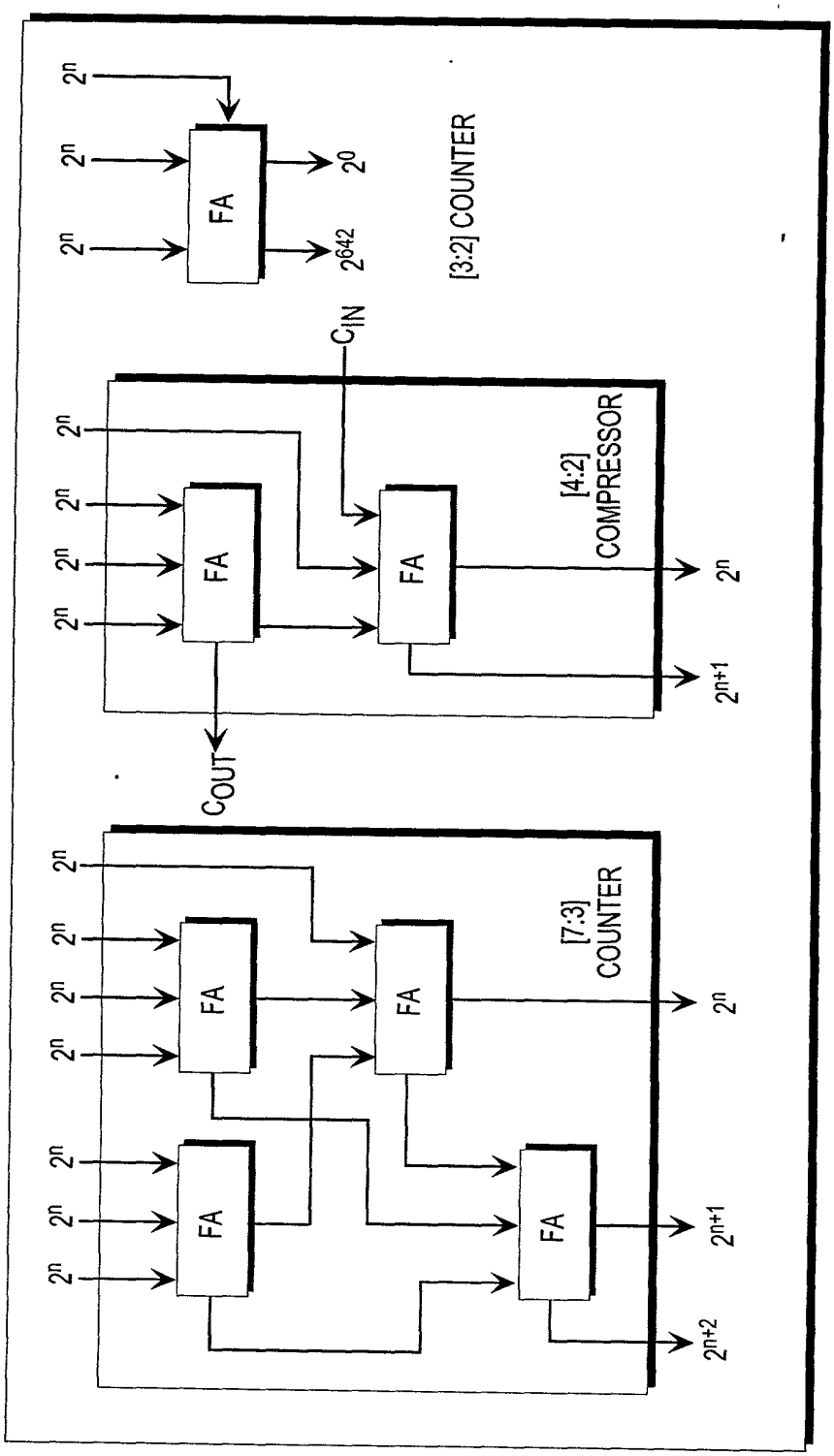

2^n
FA
2^0
2^642
[3:2] COUNTER
C_IN
[4:2] COMPRESSOR
2^n+1
C_OUT
[7:3] COUNTER
2^n+2

FIG. 16

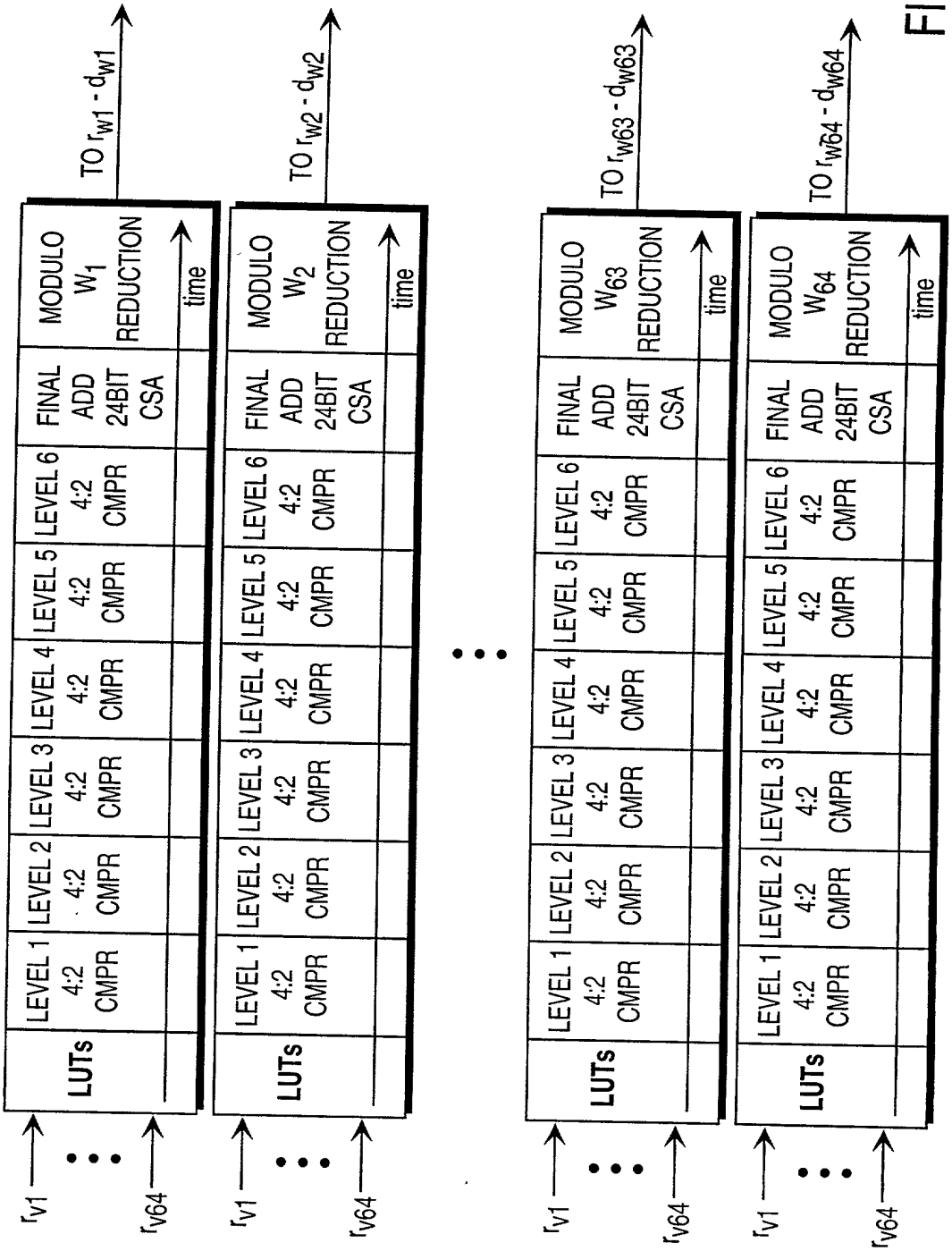

LUTs
LEVEL 1 4:2 CMPR
LEVEL 2 4:2 CMPR
LEVEL 3 4:2 CMPR
LEVEL 4 4:2 CMPR
LEVEL 5 4:2 CMPR
LEVEL 6 4:2 CMPR
FINAL ADD 24BIT CSA
MODULO W_1 REDUCTION
MODULO W_2 REDUCTION
MODULO W_{63} REDUCTION
MODULO W_{64} REDUCTION
time
r_{v1}
r_{v64}
TO $r_{w1} - d_{w1}$
TO $r_{w2} - d_{w2}$
TO $r_{w63} - d_{w63}$
TO $r_{w64} - d_{w64}$

FIG. 17

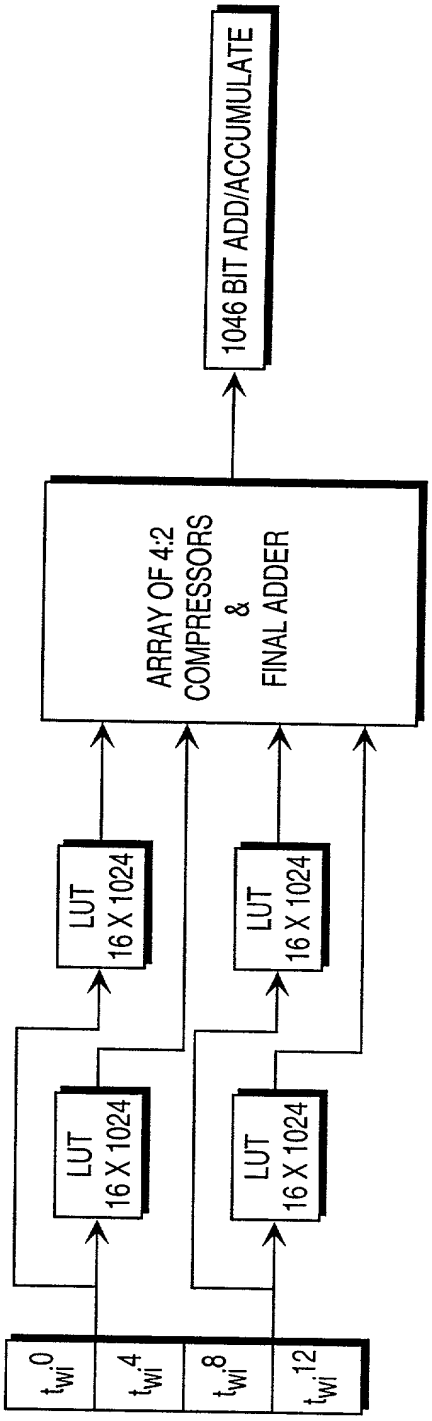


FIG. 18

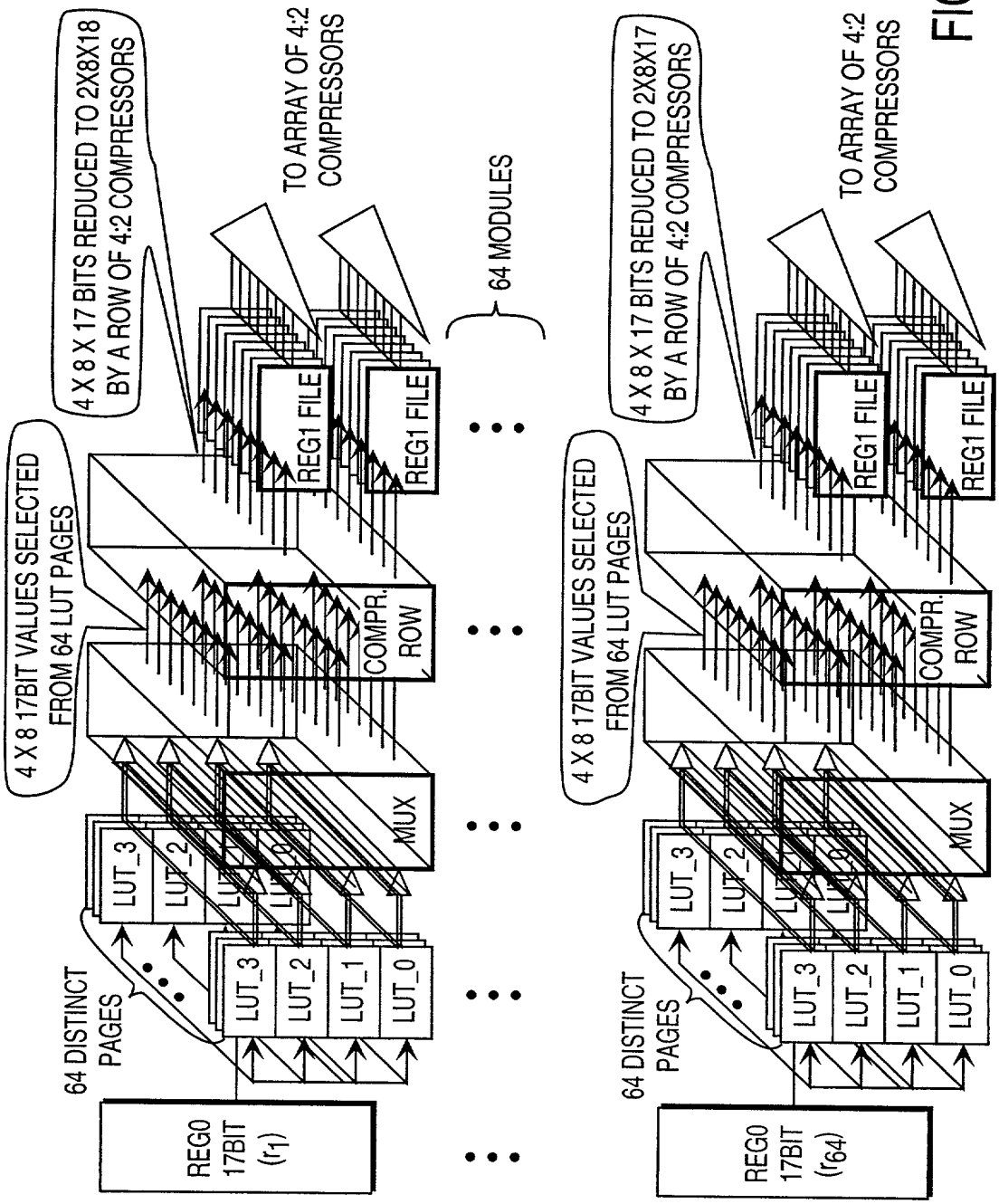

4 X 8 17BIT VALUES SELECTED FROM 64 LUT PAGES
4 X 8 X 17 BITS REDUCED TO 2X8X18 BY A ROW OF 4:2 COMPRESSORS
TO ARRAY OF 4:2 COMPRESSORS
64 MODULES
64 DISTINCT PAGES
REG0 17BIT (r_1)
LUT_3
LUT_2
LUT_1
LUT_0
MUX
COMPR. ROW
REG1 FILE
4 X 8 17BIT VALUES SELECTED FROM 64 LUT PAGES
4 X 8 X 17 BITS REDUCED TO 2X8X17 BY A ROW OF 4:2 COMPRESSORS
TO ARRAY OF 4:2 COMPRESSORS
64 DISTINCT PAGES
REG0 17BIT (r_{64})

FIG. 19

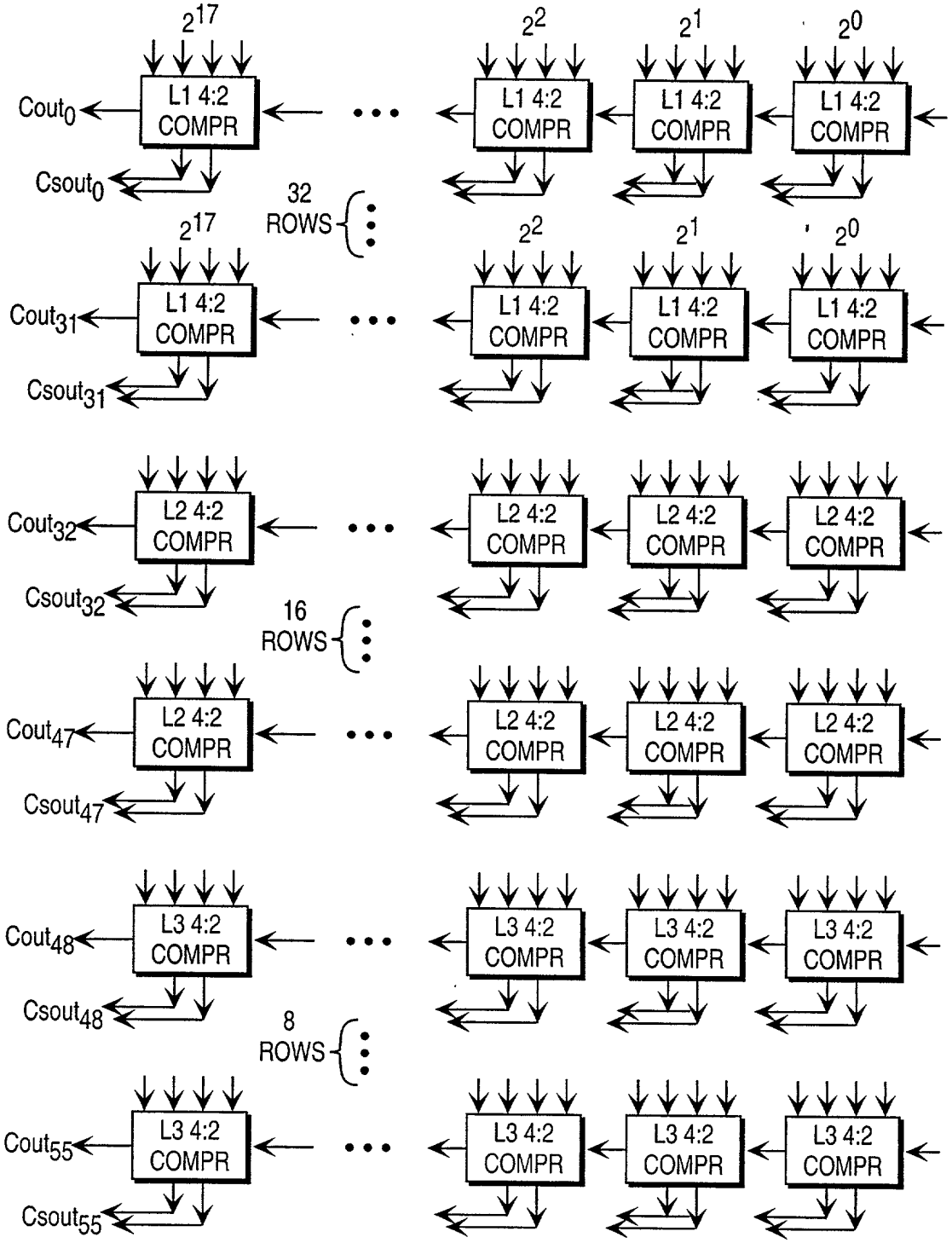


FIG. 20A

CONTINUED ON FIG. 20B

CONTINUED FROM FIG. 20A

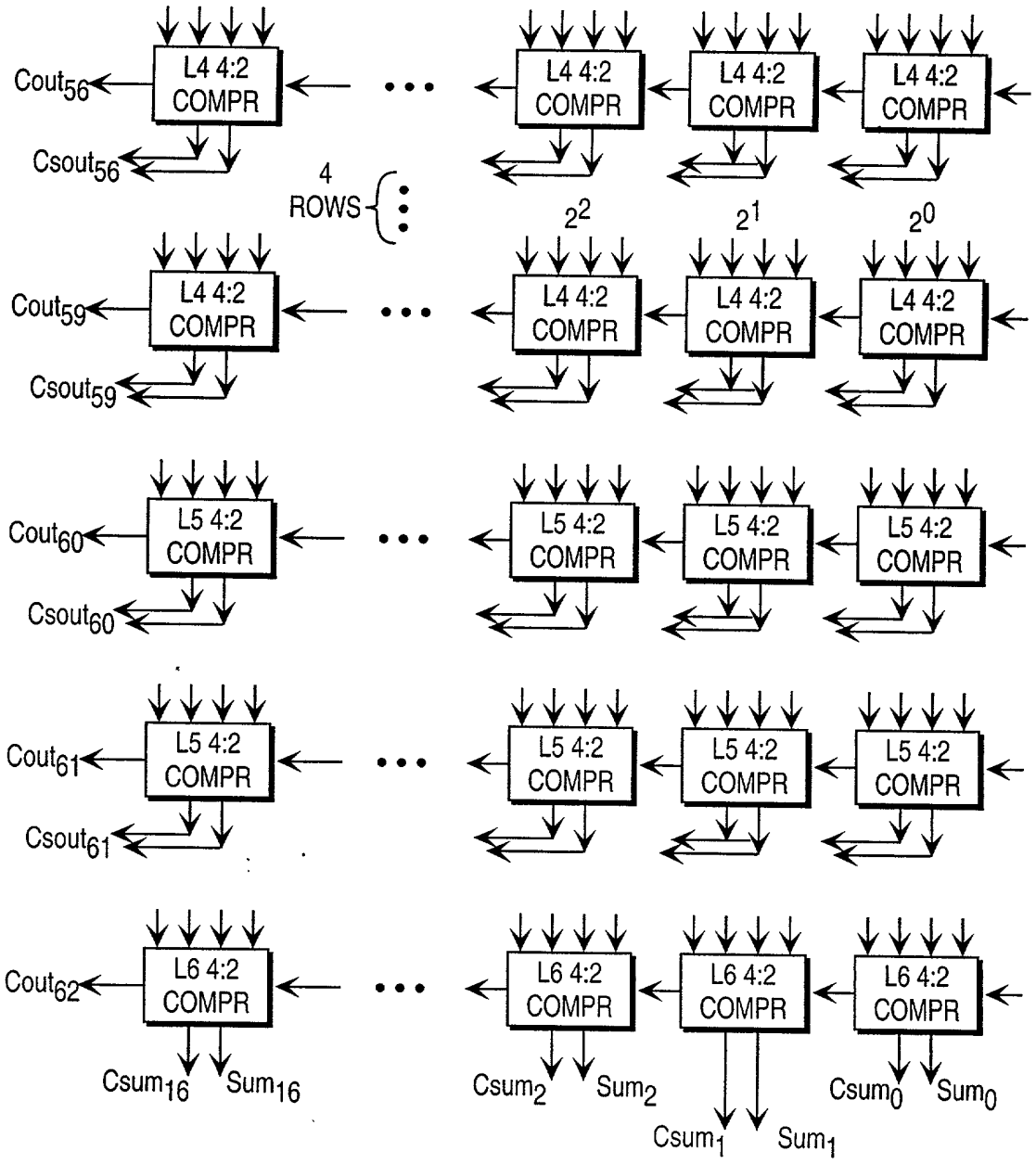


FIG. 20B

Title: Pre-Computation and Dual-Pass Modular Arithmetic Operation Approach to Implement Enc.,p.:.. F..tocols Efficiently in Electronic Integrated Circuits
Inventor(s): Mihailo M. Stojancic, et al.
Serial No.: 09/955,902
Docket No. 50325-0550

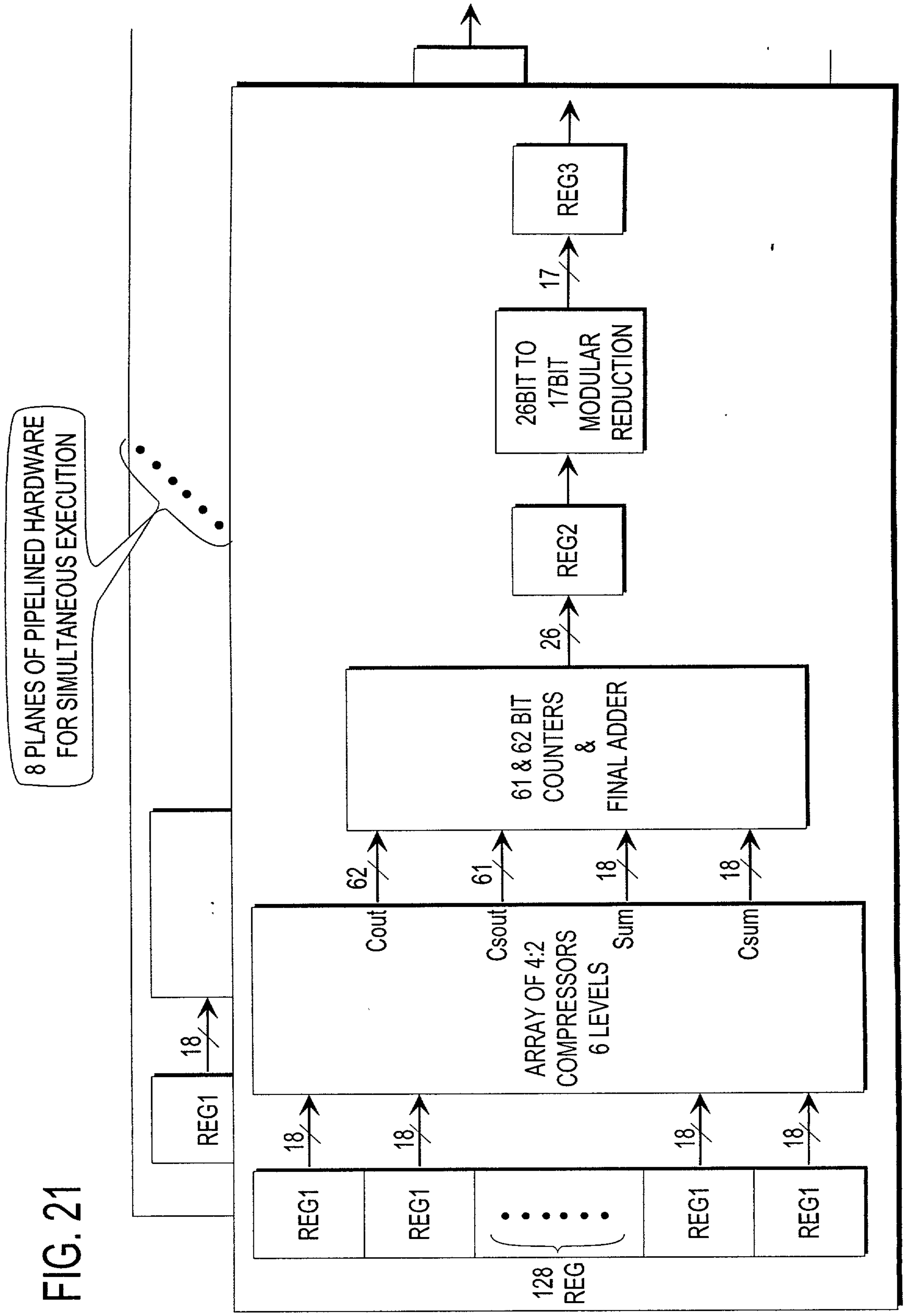
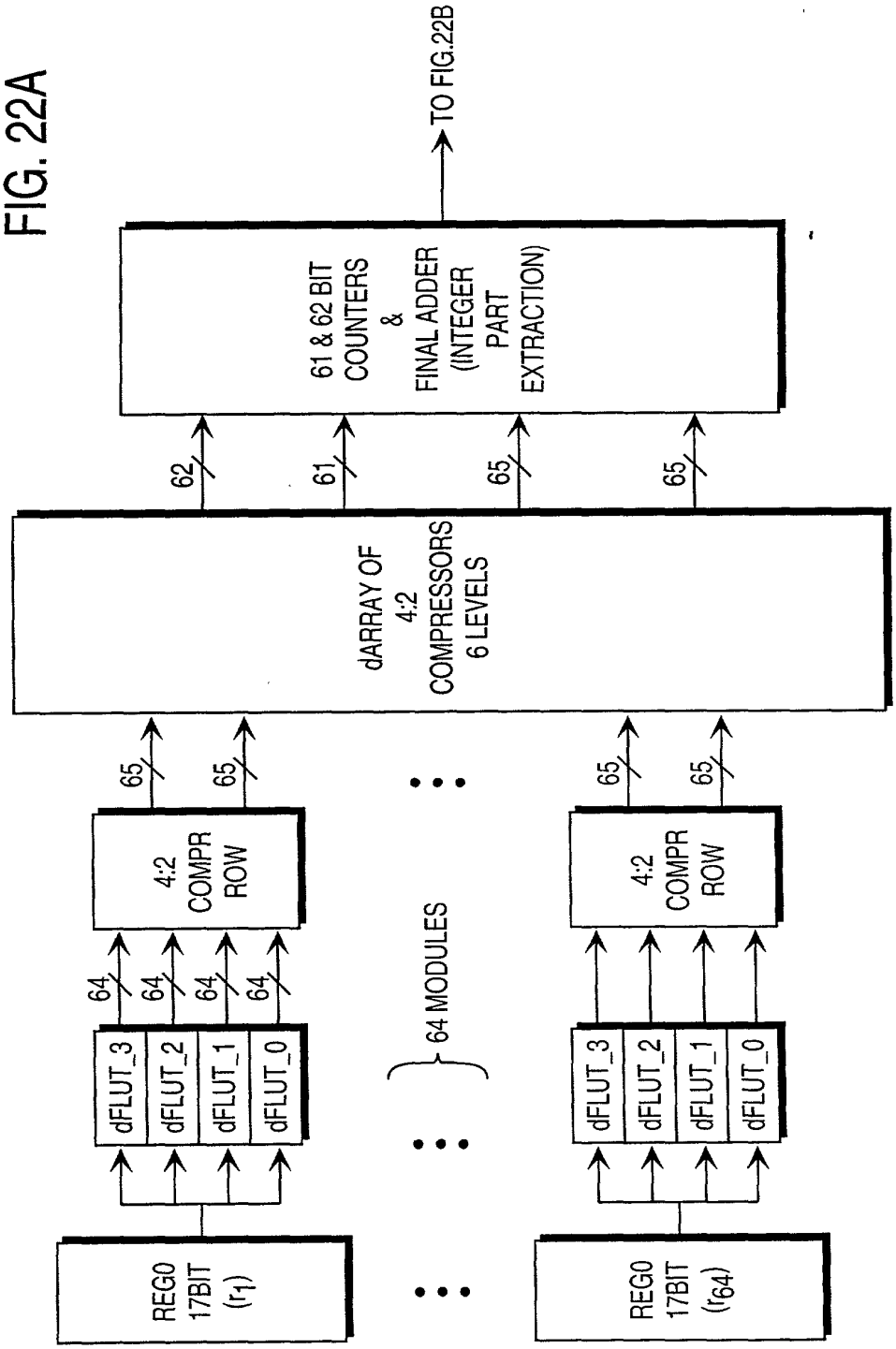


FIG. 21

FIG. 22A



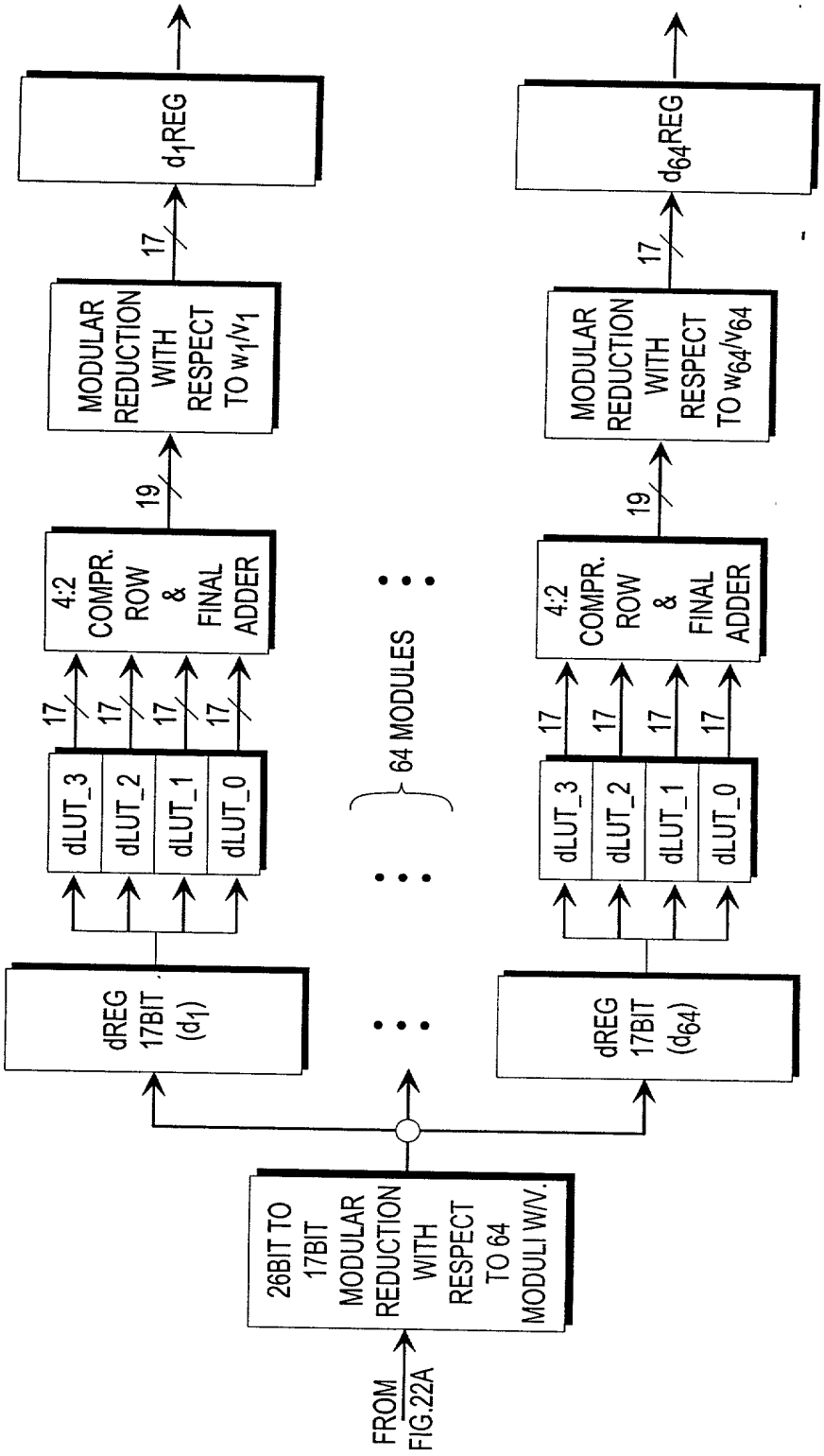


FIG. 22B

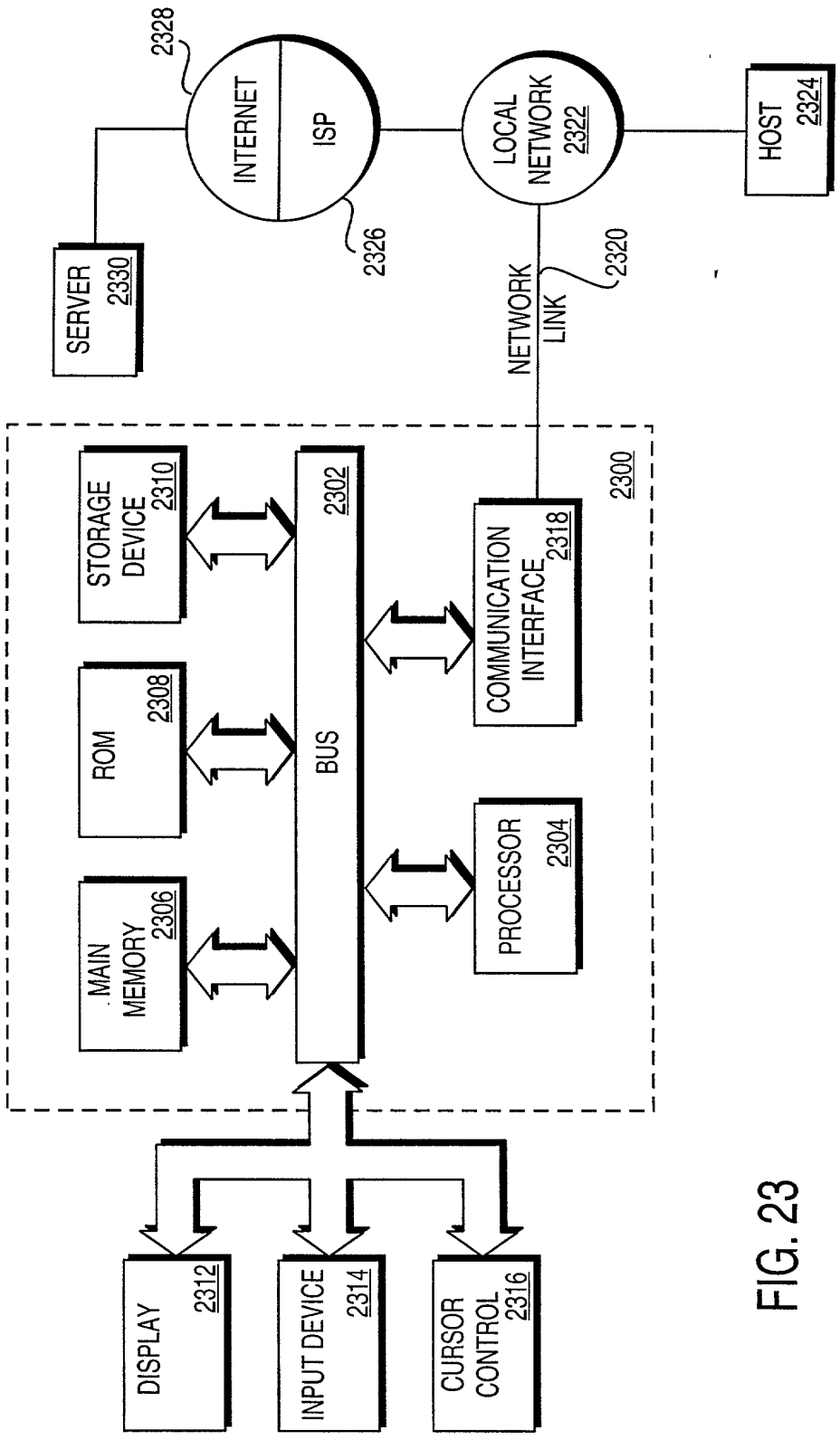


FIG. 23